UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/685,285 | 10/10/2000 | John M. Hammer | 05456.105008 | 4449 |

7590 09/07/2006

Steven P Wigmore Esq
King & Spalding
191 Peachtree Street NE
45th Floor
Atlanta, GA 30303

| EXAMINER | |
|---|---|
| HA, LEYNNA A | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

DATE MAILED: 09/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/685,285 | HAMMER ET AL. | |
| | Examiner | Art Unit | |
| | LEYNNA T. HA | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *13 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-9 and 11-65* is/are pending in the application.

4a) Of the above claim(s) *10* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9 and 11-65* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-9 and 11-65 are pending.

Claim 10 is cancelled.

### *Continued Examination Under 37 CFR 1.114*

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on June 13, 2006 has been entered.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**3. Claims 1-9 and 11-50, and 56-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack, et al. (US 6,298,445), and further in view of Trcka, et al. (US 6,453,345).**

**As per claim 1:**

Shostack, et al. disclose a method for automatically creating a record for one or more security incidents and reactions thereto, comprising the steps of:

recording computer security incident information **[col.2, lines 62-63 and col.13, lines 42-43]** [*with at least one of a date and time stamp*], the computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network **[col.4, lines 47-50 and col.5, lines 20-50]** that occur prior to a computer security threat **[col.7, lines 13-17]** and an actual computer security threat; **[col.4, lines 50-53]**

classifying the computer security incident information; **[col.9, lines 59-67]**

automatically suggesting a computer security threat the procedure based on a classification of the computer security incident information; **[col.11, lines 52-54]**

providing data to enable display of a computer security threat procedure **[col.12, lines 14-25 and 41-47]** comprising one or more steps for one of investigating and responding to the computer security incident information; **[col.6, lines 58]**

receiving a selection of one or more steps of a computer security threat procedure; **[col.8, lines 2-3 and col.11, lines 49-51]**

executing the selected one or more steps of the procedure; **[col.7, lines 56-57]**

in response to executing the one or more steps of the selected computer security threat procedure, recording executed computer security threat procedure information and results of the executed one or more steps of the computer security threat procedure **[*with at least one of a date and time stamp; and*]** **[col.7, lines 25-27]**

outputting a record comprising the computer security incident information, executed computer security threat procedure information, results of one or more steps of the executed computer security threat procedure **[col.13, lines 15-17 and 31-36]**, an identity of a user who selected the computer security threat procedure **[col.9, lines 16-17 and 56-63]**, and at least one of a corresponding **[*date and time stamp*]**.

However, Shostack did not include a date and time stamp.

Trcka, et al. discloses an invention that provides a network security and analysis system, which includes a variety of features for automatically and interactively monitoring and analyzing traffic (col.2, lines 11-15 and col.11, lines

1-4). Trcka discloses utilizes archival recordings to evaluate security breaches and other anomalies (col.7, lines 49-50). The archival recordings can be used to perform a wide range of network analysis and restoration tasks that includes checking for newly discovered viruses and performing low-level analysis of network break-ins (col.2, lines 56-61). Further, Trcka discusses the date/time stamp reflects the dates and times that the packets are transmitted on the network (col.15, lines 55-57). Thus, preserve the details of the original timing of the traffic on the network and to facilitate the subsequent reconstruction of network events (col.7, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of recording computer security incident information and the computer security threat procedure as taught by Shostack with at least one of a date and time stamp as taught by Trcka because this preserves the original timing of the traffic on the network and facilitates subsequent reconstruction of network events (col.7, lines 10-12 and col.14, lines 34-36).

**As per claim 2:** **see Trcka on col.7, lines 1-3;** discussing an unmodifiable permanent database.

**As per claim 3:** **see Shostack on col.11, lines 5-17 and col.13, lines 50-55;** discussing the step of recording the results of the executed computer security threat procedure with a digital signature to enable detection of any modification of the recorded results, whereby integrity of the recorded results can be monitored.

**As per claim 4:** **see Shostack on col.7, lines 55-60 and col.10, lines 50-54;** discusses extracting the information from the results of an executed computer security threat procedure.

**As per claim 5:** **see Shostack on col.7, lines 14-27 and col.10, lines 50-54;** discusses describing a computer security incident with said extraction information.

**As per claim 6:** **see Shostack on col.12, lines 14-25 and 41-47;** discussing displaying information for a particular computer security incident to more than one user.

**As per claim 7:** **see Shostack on col.13, lines 7-17;** discusses prepopulating fields of a record of a first program module from a second program module.

**As per claim 8:** **see Shostack on col.7, lines 10-29;** discusses receiving security incident information from a first program module; processing the security incident information with a second program module; and forwarding the processed computer security incident information from the second program module to a third program module.

**As per claim 9:** **see Shostack on col.11, lines 52-54;** discusses receiving a selection of a computer security threat procedure comprises automatically selecting a computer security threat procedure with a program module.

**As per claim 10:** **Cancelled**

**As per claim 11:** **see Shostack on col.11, lines 52-54;** discussing each steps are performed automatically by a program module.

**As per claim 12: see Shostack on col.11, lines 52-54;** discussing some steps are performed automatically by a program module.

**As per claim 13: see Shostack on col.13, lines 7-17;** discusses displaying reports comprising one or more computer security incidents.

**As per claim 14: see Shostack on col.12, lines 46-47;** discussing the results of an executed procedure comprises at least one of text, numbers, images, or formatted documents.

**As per claim 15: see Shostack on col.7, lines 13-15;** discusses predicting future actions of a source of a computer security incident.

**As per claim 16: see Shostack on col.5, lines 21-61;** discusses identifying the source of a computer security incident.

**As per claim 17: see Shostack on col.6, lines 42-46;** discusses sorting decoy or false security incidents from actual computer security incidents.

**As per claim 18: see Shostack on col.7, lines 25-29 and col.11, lines 50-51;** discusses linking a first computer security threat procedure to a second computer security threat procedure.

**As per claim 19: see Shostack on col.12, lines 58-65;** discusses determining the authorization level of a user.

**As per claim 20: see Shostack on col.8, lines 63-67 and col.12, lines 14-25 and 41-47;** discusses providing data to enable display of a computer security threat procedure further comprises the step of providing data for enabling display of one or more steps of a computer security threat procedure.

**As per claim 21: see Shostack on col.8, lines 63-67 and col.12, lines 14-25 and 41-47;** discusses providing data to enable display of a computer security threat response procedure; executing the computer security threat response procedure; **[col.7, lines 56-57]** and in response to executing the response computer security threat procedure, recording executed computer security threat response procedure information and results of the executed computer security threat response procedure **[col.7, lines 25-27 and col.13, lines 15-17 and 31-36]** **[***with at least one of a date and time stamp* ***(See Trcka on* col.7, lines 10-12 and col.14, lines 34-36 and col.15, lines 55-57). ]**.

**As per claim 22: see Shostack on col.8, lines 63-67 and col.12, lines 14-25 and 41-47;** discusses providing data to enable display of a computer security threat investigation procedure; executing the computer security threat response procedure; and in response to executing computer security threat investigation procedure **[col.7, lines 56-57];** and recording executed computer security threat response procedure information and results of the executed computer security threat response procedure **[col.7, lines 25-27 and col.13, lines 15-17 and 31-36]** **[***with at least one of a date and time stamp* ***(See Trcka on* col.7, lines 10-12 and col.14, lines 34-36 and col.15, lines 55-57)]**.

**As per claim 23: see Shostack on col.8, lines 63-67 and col.12, lines 14-25 and 41-47;** discusses providing data to enable display of the computer security threat response procedure further comprises the step of providing data to enable display of one or more steps of the computer security threat response procedure.

**As per claim 24: see Shostack on col.8, lines 63-67 and col.12, lines 14-25 and 41-47;** discusses providing data to enable display of results of the executed computer security threat procedure.

**As per claim 25: see Shostack on col.7, lines 24-29 and col.11, lines 50-54;** discusses providing data to enable display of results of the executed computer security threat procedure.

**As per claim 26: see Shostack on col.7, lines 24-29 and col.11, lines 50-54;** discusses identifying an appropriate computer to execute a step in the computer security threat investigation procedure; and identifying an appropriate computer to execute a step in the computer security threat response procedure.

**As per claim 27: see Shostack on col.10, lines 52-60 and Trcka on col.7, lines 60-63;** discusses accessing a table comprising computer locations and step information; comparing a step to be executed with computer locations listed in the table; determining if a match exists between the step to be executed and the computer locations; and if one or more matches exist, displaying the matching information or automatically selecting appropriate location.

**As per claim 28: see Trcka on col.7, lines 60-63 and col.18, lines 1-14;** discussing the table further comprises Internet address ranges, the method further comprising the step of comparing an Internet address of a source of a computer security incident with the Internet address ranges of the table.

**As per claim 29: see Trcka on col.15, lines 50-54;** discusses providing data to enable display of an appropriate substitute computer location if a match does not exist.

**As per claim 30: see Shostack on col.6, lines 58;** discusses identifying an appropriate computer to execute a step in either an investigation or a computer security threat response procedure, wherein the computer is strategically located relative to a source of a security incident.

**As per claim 31: see Shostack on col.7, lines 55-64;** discusses executing one or more program modules in response to a selection of a computer security threat procedure.

**As per claim 32: see Shostack on col.7, lines 55-64;** discussing one or more program modules comprises one or more software application programs that can operate as a stand-alone programs.

**As per claim 33: see Shostack on col.7, lines 55-64;** discussing one or more program modules comprises an off the shelf software application programs.

**As per claim 34: see Shostack on col.9, lines 58-67;** discussing the security incident information comprises predefined attributes.

**As per claim 35: see Trcka on col.7, lines 60-63 and col.18, lines 1-14;** discussing the predefined attributes comprise any one of a computer incident severity level, a computer incident category, a computer incident scope value, a computer incident status value, an attacker internet protocol (IP) address value, an attacker ISP name, an attacker country, an external attacker status value, an incident type value, a vulnerabilities level, an entry point value, an attack profile value, a target networks value, a target firewalls value, a target hosts value, a target services value, a target accounts value, and a damage type value.

**As per claim 36:** **see Shostack on col.9, lines 58-67;** discussing the security incident information comprises attributes that are at least one of variable and computer-generated.

**As per claim 37:** **see Shostack on col.9, lines 58-col.10, line 9;** discusses whether a computer security incident comprises an actual breach in security based upon values of its attributes.

**As per claim 38:** **see Shostack on col.6, lines 42-58;** discusses receiving a selection for a step of a computer security threat procedure; and generating a pre-execution warning prior to the selection of a step.

**As per claim 39:** **see Shostack on col.6, lines 42-58 and col.7, lines 24-29;** discusses receiving a selection for a step of a computer security threat procedure, executing the selected step, and suggesting an appropriate subsequent step in the computer security threat procedure.

**As per claim 40:** **see Shostack on col.11, lines 52-54;** discussing each step is performed automatically in response to a detected computer security incident.

**As per claim 41:** **see Shostack on col.12, lines 14-48;** discusses providing data to enable display of a plurality of computer tools in a non-procedural manner; receiving a selected for a computer tool; and executing the selected computer tool.

**As per claim 42:**

Shostack, et al. disclose a method for organizing and recording reactions to one or more security incidents, comprising the steps of:

classifying the computer security incident information; **[col.9, lines 59-67]**

automatically suggesting one or more computer security threat investigation procedure based on a classification of the computer security incident information; **[col.11, lines 52-54]**

providing data to enable display of one or more computer security threat investigation procedures **[col.12, lines 14-25]** for investigating one of suspicious computer activity **[col.6, lines 58]** that occur prior to a computer security threat and an actual computer security threat; **[col.4, lines 50-53]**

providing data to enable display of the one or more computer security threat response procedures for responding to one of suspicious computer activity comprising one or more attacks received from a network computer **[col.7, lines 13-15]** that occur prior to a computer security threat and an actual computer security threat; **[col.12, lines 41-47]**

in response to a selection of a computer security threat investigation procedure, providing data to enable display of one or more corresponding investigation steps; **[col.7, lines 45-46 and col.8, lines 65-67]**

in response to a selection of a computer security threat response procedure, providing data to enable display of one or more corresponding response steps; and **[col.8, lines 2-3 and col.11, lines 49-51]**

generating a permanent record comprising security incident information, executed investigation step and result information, executed response step and result information **[col.7, lines 25-27 and col.13, lines 15-17 and 31-36]**, and **[*corresponding date and time stamp*]**.

However, Shostack did not include a date and time stamp.

Trcka, et al. discloses an invention that provides a network security and analysis system, which includes a variety of features for automatically and interactively monitoring and analyzing traffic (col.2, lines 11-15 and col.11, lines 1-4). Trcka discloses utilizes archival recordings to evaluate security breaches and other anomalies (col.7, lines 49-50). The archival recordings can be used to perform a wide range of network analysis and restoration tasks that includes checking for newly discovered viruses and performing low-level analysis of network break-ins (col.2, lines 56-61). Further, Trcka discusses the date/time stamp reflects the dates and times that the packets are transmitted on the network (col.15, lines 55-57). Thus, preserve the details of the original timing of the traffic on the network and to facilitate the subsequent reconstruction of network events (col.7, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of recording computer security incident information and the computer security threat procedure as taught by Shostack with at least one of a date and time stamp as taught by Trcka because this preserves the original timing of the traffic on the network and facilitates subsequent reconstruction of network events (col.7, lines 10-12 and col.14, lines 34-36).

**As per claim 43: see Shostack on col.7, lines 24-29 and col.11, lines 50-54;** discussing recording executed investigation step information and results of the executed investigation step **[*with at least one of a date and time stamp (See Trcka on* col.7, lines 10-12 and col.14, lines 34-36 and col.15, lines 55-57)]**

in response to a selection of a step of a computer security threat investigation procedure.

**As per claim 44: see Shostack on col.7, lines 24-29 and col.13, lines 15-17 and 31-36;** discussing recording executed response step information and results of the executed response step [*with at least one of a date and time stamp (**See Trcka on** **col.7, lines 10-12 and col.14, lines 34-36 and col.15, lines 55-57)***] in response to a selection of a step of a computer security threat response procedure.

**As per claim 45: see Shostack on col.12, lines 14-48 and col.13, lines 6-17;** discusses providing data to enable display of a plurality of a computer security threat procedures; in response to receiving a selection of a computer security threat procedure, displaying a plurality of steps; obtaining modification information for the selected computer security threat procedure; and storing the modification information.

**As per claim 46: see Shostack on col.7, lines 24-29;** discusses adding or deleting a step in a procedure.

**As per claim 47: see Shostack on col.12, lines 14-48 and col.13, lines 6-17;** discusses providing data to enable display of a plurality of steps of a computer security threat procedure; in response to receiving a selection of a step, providing data to enable display of detailed information fields related to the selected step; obtaining modification information for the selected step; and storing the modification information.

**As per claim 48: see Shostack on col.7, lines 24-29;** discusses adding, deleting or modifying a step in a computer security threat procedure.

**As per claim 49: see Shostack on col.7, lines 24-29and col.12, lines 14-48;** discusses obtaining computer security incident search information and providing data to enable display of a plurality of one or more computer security incidents matching the computer security incident search information.

**As per claim 50: see Trcka on col.7, lines 10-12 and col.14, lines 34-36 and col.15, lines 55-57;** discusses tracking multiple computer security incidents and storing information for each computer security in accordance with at least one of a date and time stamp.

**As per claim 56:**

Shostack discloses a method for generating a permanent record or one or more computer security incidents and reactions thereto, comprising the steps of:

receiving the computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network that occur prior to a computer security threat and an actual computer security threat;

classifying the computer security incident information; **[col.9, lines 59-67]**

displaying one or more tools for one of investigating one of suspicious computer activity that occurs prior to a computer security threat **[col.7, lines 13-17]** and an actual computer security threat; **[col.4, lines 50-53]**

automatically suggesting a tool based on a classification of the computer security incident information; **[col.11, lines 52-54]**

receiving a selection of a tool; in response to a selection of a tool, forwarding data for execution of the tool; and **[col.8, lines 2-3 and col.11, lines 49-51]**

forwarding data for generating a permanent record comprising computer security incident information, executed tool information **[col.7, lines 25-27 and col.13, lines 15-17 and 31-36]**, and **[*corresponding date and time stamp*]**

However, Shostack did not include a date and time stamp.

Trcka, et al. discloses an invention that provides a network security and analysis system, which includes a variety of features for automatically and interactively monitoring and analyzing traffic (col.2, lines 11-15 and col.11, lines 1-4). Trcka discloses utilizes archival recordings to evaluate security breaches and other anomalies (col.7, lines 49-50). The archival recordings can be used to perform a wide range of network analysis and restoration tasks that includes checking for newly discovered viruses and performing low-level analysis of network break-ins (col.2, lines 56-61). Further, Trcka discusses the date/time stamp reflects the dates and times that the packets are transmitted on the network (col.15, lines 55-57). Thus, preserve the details of the original timing of the traffic on the network and to facilitate the subsequent reconstruction of network events (col.7, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of recording computer security incident information and the computer security threat procedure as taught by Shostack with at least one of a date and time stamp as taught by Trcka

because this preserves the original timing of the traffic on the network and facilitates subsequent reconstruction of network events (col.7, lines 10-12 and col.14, lines 34-36).

**As per claim 57: see Shostack on col.12, lines 14-48;** discusses displaying the tools as icons on a computer display.

**As per claim 58: see Shostack on col.12, lines 14-48;** discusses displaying a plurality of tools that are selectable from a menu.

**As per claim 59: see Shostack on col.10, lines 11-25;** discusses installing the one or more program modules within a single program on a server.

**As per claim 60: see Shostack on col.10, lines 11-25;** discusses installing the one or more program modules on a single server.

**As per claim 61: see Shostack on col.11, lines 41-43;** discusses installing the one or more program modules on a computer that is a target of a computer incident.

**As per claim 62: see Shostack on col.10, lines 11-25;** discusses installing the one or more program modules on both a computer that is a target of a computer incident and a server.

**As per claim 63: see Trcka on col.7, lines 60-63 and col.18, lines 1-14;** discussing comparing an Internet address of a computer subject to an attack or a security breach with the Internet address ranges of the table.

**As per claim 64: see Trcka on col.7, lines 60-63 and col.18, lines 1-14;** discussing comparing an Internet address of a witness to a computer security incident with the Internet address ranges of the table.

**As per claim 65: see Trcka on col.7, lines 60-63 and col.18, lines 1-14;** discussing comparing an Internet address of an accomplice to a computer security incident with the Internet address ranges of the table.

**4. Claims 51-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reps, et al. (US 6,070,190), and further in view of Shostack, et al. (US 6,298,445).**

**As per claim 51:**

Reps, et al. discloses a method for selecting a computer that is strategically located relative to a source of a security incident, comprising the steps of:

accessing a table comprising computer, Internet address ranges associated with the computer locations **[see col.5, lines 46-48 and col.11, lines 51-52]**, and computer security step information associated with the computer locations, the computer security step information for one of investigating **[see col.17, lines 60-67 and col.23, lines 28-35]** and responding to one of suspicious computer activity **[col.14, lines 62 – col.15, lines 3]** comprising one or more [attacks] received from a network **[col.11, lines 28-34 and col.12, lines 8-10]** that

occur prior to a computer security threat **[see col.14, lines 55-57 col.15, lines 37-56 and col.16, lines 12-65]** and an actual computer security threat; **[see col.14, lines 55-57]**, the computer location identifying devices that are able to perform the computer security step information; **[see col.24, lines 48-66]**

comparing a computer security step to be executed and a target Internet address **[col.11, lines 47-59]** with computer locations and Internet address ranges listed in the table; **[col.14, lines 25-67 and col. 25, lines 15-32]**

determining if a match exists between the computer security step to be executed and the computer locations; **[col.23, lines 27-48 and col.25, lines 39-42]**

determining if a match exists between an Internet address of a computer security incident and Internet address ranges listed in the table; and **[col.25, lines 31-37]**

[automatically selecting a computer to execute the computer security step based upon the matching step,] wherein the computer has a location and is capable of interacting with the Internet address of the security incident. **[col.11, lines 23-65 and col.25, lines 39-43]**

Although, Reps teaches monitoring for violation and support problem determination and remediation steps for the detected violation. Reps did not include monitoring, problem determination and remediation steps for attacks and also did not include automatically selecting a computer to execute the computer security step.

Shostack, et al. teaches the invention of automatically creating a record for one or more security incidents and reactions thereto, comprising the steps of

recording computer security incident information [col.2, lines 62-63 and col.13, lines 42-43], the computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network [col.4, lines 47-50 and col.5, lines 20-50] that occur prior to a computer security threat [col.7, lines 13-17] and an actual computer security threat [col.4, lines 50-53] and classifying the computer security incident information [col.9, lines 59-67]. Shostack discloses providing data to enable display of a computer security threat procedure [col.12, lines 14-25 and 41-47] comprising one or more steps for one of investigating and responding to the computer security incident information [col.6, lines 58] whereby receiving a selection of one or more steps of a computer security threat procedure; [col.7, lines 25-27 and col.8, lines 2-3] and recording executed computer security threat procedure information and results of the executed one or more steps of the computer security threat procedure [col.11, lines 49-51]. Shostack discloses automatically may implement the suggested repairs of the system vulnerabilities [col.11, lines 52-54]. By automatically providing enhancements to a data of security vulnerabilities and using that information to provide security solutions to potentially weak computers (col.4, lines 9-13).

Therefore it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of monitoring, problem determination, and remediation steps of Rep for attacks and to automatically implement suggested repairs as taught by Shostack because this prevents unauthorized access to the network such that the techniques for

breaching computer security have been reported and discovered to automatically provide appropriate solution before a breach occurs (col.7, lines 24-27 and 45-46) even for newly discovered attacks (col.11, lines 50-53).

**As per claim 52:** **see Reps on col.9, lines 24-35;** discusses if one or more matches exist, providing data to enable display of the matching information and if a match does not exist, providing data to enable display of one or more appropriate substitute computer location or automatically selecting an appropriate location.

**As per claim 53:** **see Reps on col.16, lines 34-67;** discusses a portion of a computer security threat response procedure, wherein the computer is strategically located relative to a source of a security incident.

**As per claim 54:** **see Reps on col.19, lines 27-46;** discusses a portion of a computer security threat investigation procedure, wherein the computer is strategically located relative to a source of a security incident.

**As per claim 55:** **see Reps on col.15, lines 7-10;** discussing one or more off the shelf security application programs.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

HOSUK SONG
PRIMARY EXAMINER